Amendments to the Specification:

Please amend paragraph [06] as follows:

More particularly, for single sign-on, a communication network offers management of user identifiers of users accessing data applications via at least two different networks. The network includes a wireless communication network providing a link to a mobile station and access to a data application associated with the wireless network. A user accessing the data application from the mobile station is identified by mobile station identifiers. The network also includes another communication network ~~other~~ that links a user interface other than the mobile station with a second data application. The user accessing the second data application from the user interface is identified by the user identifier entered by the user. A computer system in communication with data applications of the wireless communication network and with the other communication network facilitates user sign-on capabilities to the data applications from the user interface with the same user identifier.

Please amend paragraph [08] as follows:

Also, the computer system is in communication with a third-party network hosting a third-party data application. A Lightweight Directory Access Protocol (LDAP) interface interfaces the third-party network with the computer system. An authorization server may be connected between the interface and the computer system, or the computer system may be configured to authenticate and authorize access to the third party data application and a data application of either the wireless or the other communication network.

Please amend paragraph [20] as follows:

~~Fig. 4 is a~~ Figs. 4A and 4B are block ~~diagram~~ diagrams of ~~another~~ other communication network ~~configuration sharing~~ configurations, which share components of the wireless communication network and web-based communication network.

Please amend paragraph [37] as follows:

Leveraging authentication of the HLR server may be carried out periodically or when a request to any particular data application is received at the AAA server. Typically, the AAA server will send a request to the HLR station, and request authenticated mobile stations currently accessing the wireless network. This data may be stored in the AAA server for future processing of access ~~request~~ requests to data applications on the network. Alternatively, the AAA server may request whether or not a particular mobile station attempting to access a data application has been authenticated by the HLR station. In either event, the AAA server leverages the HLR authentication so as to authorize or prohibit access to a data application by a user accessing via a mobile station. Thus, instead of providing a username/password combination to the data application, the network takes advantage of mobile station identifiers which have been processed by the corresponding HLR in order to determine whether or not a mobile station and user is permitted to access a particular data application.

Please amend paragraph [42] as follows:

Authentication and Authorization may be carried out simultaneously or at different times. If the AAA server that ~~leverager~~ leverages authentication information from the HLR also performs authorization, the AAA server may perform Authentication and Authorization for the user generally at the same time. In other words, when the AAA server authenticates a user with received mobile station identifiers, authorization information may be performed at the same time.

Please amend paragraph [46] as follows:

Fig. [[2]] 2A illustrates two data applications (X and Y), which embody any type of data application accessible over the internet. For discussion purposes, applications X and Y represent data applications accessible via the internet for sending data to the station user, e.g., on their personal computer 204, or to their mobile station 110 as set up by the user. On the internet, many such applications are deployed by many different parties and are accessible from both mobile and landline user terminals. For purposes of this discussion, it is assumed that applications X and Y are deployed by the same service provider or an associated party provides applications X and Y. Typical examples of data applications X and Y include text messaging services, and any other type of application which is customizable by accessing the application over the internet 208. Applications A and B, which relate to mobile services, may be accessible via this user interface 204 as well. The user may manage his/her profile, update account information, purchase upgrades, etc.

Please amend paragraph [50] as follows:

Referring to Figs. ~~2B-D~~ 2B-C, each product server XPS, YPS, hosting data applications X, Y respectively, communicate with a database 210 for storing user identifiers, user profile information, and any other types of information associated with the user. This database 210 may be located on the same product server of the respective data application X and Y, as shown in Fig. 2B, or may be located on a different product

Please amend paragraph [60] as follows:

In each configuration, the server or group of servers maintaining user identifiers is generally referred to as a "computer system" 314. If using a combination of servers as Fig. 3C illustrates, preferably, the AAA server 316 authenticates and ~~authorization~~ authorizes mobile stations over the radio network 100, and the other server 310 authenticates and authorizes other devices accessing applications over a web-based network 312. The AAA server 136 periodically connects to database 310 and downloads, new, updated or changed user identifiers, after which time user identifiers are removed from the database 310. In this manner, a service provider can easily update a system to accommodate single sign-on capabilities. From the user standpoint, there is no change.